



| | |
|--|--|
| Westchester County Information Technology Policy | No: WC-P08-001 |
| IT Policy: Security & Technology Use Policy | Updated: 11/1/2022 |
| | Issued By: Westchester County Department of Information Technology (DoIT) |
| | Owner: Marguerite Beirne Chief Information Officer mcb1@westchestergov.com |

1. Purpose

Information and information systems are key assets of Westchester County ("the County"). They are essential to the conduct of County business and are a part of most employees' daily work. The County provides systems, including the computers, networks, technology applications and the information housed therein to permit employees to perform their duties more effectively.

This policy sets forth a basic set of standards for use and protection of computer and information assets. It includes but is not limited to computer workstations, laptop computers, smartphones, electronic mail ("e-mail"), databases, networks and connection(s) – both wired and wireless – to the intranet, Internet and any other information technology services available both now and in the future.

Inappropriate use of equipment and services exposes the County to risks including virus attacks, system compromise, interruption of services and legal issues.

Effective security is a team effort involving the participation and support of every County employee and affiliate who deals with data and / or information systems. It is the responsibility of every computer user to know these guidelines and to conduct activities accordingly.

2. Authority

The Charter and Administrative Code of Westchester County, NY provides the Department of Information Technology (DoIT) with the authority to establish countywide technology policies, including technology and security standards. The County's Chief Information Officer has the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for County government, including hardware, software, security and business re-engineering.

3. Scope/Responsibilities

This policy covers all employees of Westchester County. It also covers any other individuals, including consultants, interns, temporaries and vendors, who have access to County technology facilities, computers or networks.

All individuals – as defined above – are responsible for complying with this policy and for immediately reporting any known or suspected violations of this policy to their immediate supervisor or the Department of Information Technology. The CIO must approve any exceptions to this policy. Requests for exceptions and the CIO's decision must be in writing and come from the appropriate Commissioner or Department Head. All employees will be required on an annual basis to acknowledge that they have read and understand this policy as part of Westchester County's Annual Compliance Training administered by the Department of Human Resources. Persons who violate this policy will be subject to appropriate disciplinary action, up to and including termination.

4. Ownership

Information processing related systems, including but not limited to: computer equipment, operating system software; application software, network accounts providing e-mail, Web browsing, File Transfer Protocol, networking and intranet hardware and software (collectively "System(s)"), are owned by or licensed by Westchester County. They are intended primarily for County business purposes.

A County employee will be given either a desktop PC or laptop PC, if there is sufficient work out of the office.

Equipment purchased by employees will not be considered a County asset or authorized to connect to the County Network or any other County assets. Further, devices not supported by DoIT will not be configured for County use. Employee procurement of devices and service must be approved by DoIT if

connectivity to County systems is required.

In the event a County or personal device is lost or stolen, it must be reported immediately to the police as well as DoIT for disablement from our systems. A copy of the police report must be provided to DoIT through a Commissioner or Department Head. Damaged devices must not be sent to retail service centers prior to IT inspection. This will eliminate the risk of any unauthorized data access.

5. Personal Use

Incidental personal use of County Systems is permissible if the use:

- 5.1. Does not consume a significant amount of resources that could otherwise be used for business purposes;
- 5.2. Does not interfere with any employee's productivity;
- 5.3. Does not preempt any business activity;
- 5.4. Is not contrary to any other County policies. It is the responsibility of each employee and manager to ensure that the County's technology is used properly.

6. Prohibited Use

Improper uses of County Systems include, but are not limited to:

- 6.1. Contributing to blogs, public forums, social media sites, chat rooms or message boards in an inappropriate way (see section below – "Social Media" – for details);
- 6.2. Misrepresenting, obscuring, suppressing or replacing any identity on an electronic communication;
- 6.3. Any use or communication in violation of other County policies, such as Equal Employment Opportunity policy, Harassment policies, etc;
- 6.4. Any use of profanity, obscenities, or suggestive, intimidating, hostile, discriminatory or derogatory remarks, even in jest;
- 6.5. Downloading of copyrighted material without specific permission of copyright owner;
- 6.6. Downloading of large files or data for personal use, including video, music, photographs, etc.;
- 6.7. The automated forwarding of messages outside of the County;
- 6.8. Engaging in any business activity outside of the County;
- 6.9. Gambling;
- 6.10. Any unauthorized test or attempt to compromise computer or communication system security;
- 6.11. Any use that violates federal, state, or local law or regulation;
- 6.12. Knowingly or recklessly disrupting the normal operation of computers,

peripherals, or networks. "Disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service and forged routing information for malicious purposes;

- 6.13. Connecting unauthorized equipment to the network for any purpose;
- 6.14. Running or installing games or any other unauthorized software on County Computers, including personal Web servers;
- 6.15. Copying of any software from County computers, for other than archiving purposes;
- 6.16. Using the County network to gain unauthorized access to any computer system;
- 6.17. Using County systems to access, transmit, store, display, or request obscene, pornographic, erotic, profane, racist, sexist, violent, drug-related or other offensive material (including messages, images, video, or sound);
- 6.18. Using County systems in such a way as to create an intimidating or hostile work environment;
- 6.19. Using County systems to solicit for personal gain or for the advancement of a political or religious belief;
- 6.20. Modifying County-issued computer software, especially anti-virus / security software.
- 6.21. Any use of personal (non-County) email to conduct County business. This includes the use of personal email (e.g., Gmail, Yahoo, Hotmail) to generate, forward or receive information/data/files in any format pertaining to County business. Use of personal email may lead to the loss of County data. As per section 6 below ("Monitoring and Privacy of Communications"), all electronic communications pertaining to County business are considered County records and subject to disclosure to law enforcement or government officials or to other third parties through FOIL (Freedom of Information Law) requests or other process;
- 6.22. Using County systems to access unauthorized third-party, cloud-based hosting solutions (e.g., Dropbox, Google Drive, etc.) to store County data outside of the County network. Further, it is not permitted to create any accounts with Dropbox or similar services using westchestergov / westchestercountyny.gov domain email accounts.

7. Social Media

Although social media technology is constantly changing, this policy was developed to cover Westchester County employee and County Network user participation in all forms of communicating or posting information or content via the Internet, including, but not limited to, social networking sites (for example, Facebook, LinkedIn), blogs, Twitter accounts, video- or photo-sharing sites, websites, chat rooms, and other forms of online dialogue.

All County employees and Network users must at a minimum adhere to the following rules when using social media technologies on County IT resources and/or in their capacities as a County employee:

- 7.1. Use of social media may not interfere with any employee's productivity or detract resources from performing assigned business related duties.
- 7.2. Social media behavior may in no way harm or tarnish the image, reputation and/or goodwill of the County and/or any of its employees.
- 7.3. Employees are prohibited from making any discriminatory, disparaging, defamatory or harassing comments when using social media or otherwise engaging in any conduct prohibited by The County's Non-Discrimination and Anti-Harassment policy.
- 7.4. Abide by all applicable policies and work rules regarding the use of the Internet when using social media tools for business and personal use. The use of social media tools on Westchester County IT resources will be monitored by the same method as defined in those policies and work rules.
- 7.5. Are responsible for all of their online activities that are: conducted with a County e-mail address; can be traced to a County domain; and/or use County resources.
- 7.6. Must not discuss or post confidential, proprietary or otherwise restricted information.
- 7.7. When speaking on behalf of the County in an official capacity, users must be transparent when participating in any online community. They should disclose their identity and affiliation with the County government entity.
- 7.8. Communicate in a professional manner.
- 7.9. Abide by copyright and other applicable laws. Participation online results in a user's comments being permanently available and open to being republished in other media. Users should be aware that libel, defamation, copyright and data protection laws apply.
- 7.10. When communicating on behalf of the County, County employees must obtain the necessary authorizations by management, the Office of Communications or other designee, as appropriate.
- 7.11. Must obtain permission before publishing photographs, videos or quotes of others. When not representing the County government entity, County employees who publish personal or professional opinions must not invoke their County government title. In such cases, users must use a disclaimer such as the following where technically feasible: "The postings on this site are my own and do not represent the position, strategy or opinion of Westchester County Government (or other County department/entity)."

Note: The complete Westchester County Social Media Policy can be found in the “Acceptable Computer Usage” folder on the Westchester County Intranet here: <https://cwww.westchestergov.com/PersonnelDoc/>

8. Monitoring and Privacy of Communications

Westchester County maintains the right to access and examine County computer systems and networks and all information that is stored or transmitted through these systems and networks, including all e-mail and website visits. All electronic communications are considered County records. As County records, electronic communications are subject to disclosure to law enforcement or government officials or to other third parties through FOIL (Freedom of Information Law) requests or other discovery process. Employees must ensure that information contained in electronic communications is accurate, appropriate and lawful.

While Westchester County does not intend to regularly review employees’ e-mail records, employees have no right or expectation of privacy in e-mail. Since the County is responsible for the servicing and protecting of its electronic communications networks and administering this policy, it is occasionally necessary to intercept or disclose electronic communication. Upon an employee’s termination, the Legal Department, Human Resources or the employee’s manager will direct his/her e-mail to be managed by another employee.

Communications on these Systems are not private. Users should be aware that the data they create on the System remains the property of the County, and usually can be recovered even though deleted by the user. Despite security precautions, there is no absolutely fail-safe way to prevent an unauthorized user from accessing stored files. The confidentiality of any information stored or transmitted on the System cannot be guaranteed. Furthermore, information that is stored on the System or sent via e-mail may be subject to disclosure pursuant to the New York State Freedom of Information Law and discovery.

9. Identification and Passwords

Each individual must be positively identified prior to being able to use any County computer or communications system resource. Positive identification for internal County networks involves a User-ID and a password, both of which is unique to an individual and will be supplied by DoIT upon employment. Each person must log off from all User-ID accounts before leaving at the end of their workday, unless instructed otherwise by DoIT.

Each person is responsible for all activity that occurs on his or her User-ID. User-

ID's will be revoked if an employee is terminated or departs County employment for any reason. New User-ID's will also be issued to employees who transfer to another department. Previous access privileges associated with the employee's User-ID (to e.g. e-mail, documents, system resources, shared folders, etc.) will be removed upon transfer. A new User-ID will then be created for the employee with appropriate access and security levels assigned to it.

Westchester County Network Password Policy

The Westchester County network password allows county employees to sign in to the county network to access PC's, use county e-mail, and/or access county shared-file resources (Shares).

Employees are required to change their network passwords **every 90 days** in order to create a more secure user and systems environment. This requirement supplements existing requirements for strong passwords, which improve our protections against malicious software and hackers.

This 90-day change policy is required in a number of data compliance regulations that offer specific guidance on handling personal information and compliance for sensitive data. It is imperative that we ensure that our information security policies and IT systems and processes comply with the guidelines.

The change in policy also allows us to better protect against various threats including escalated and persistent phishing attacks that we are seeing regularly. A phishing attack is malicious activity conceived by individuals who hope users will divulge personal information such as credit card numbers, passwords and security codes. As time goes on, it is becoming increasingly difficult to ascertain if some notices for information are real or are phishing, because the individuals doing it are getting better and better. As a result, the county is taking precautions to stave them off.

Important: Remember that DoIT will never ask you to divulge your password on the phone or in an online form or in an e-mail. The only place that you should enter your password is within the applications your use to perform county functions. Follow these two steps when you receive a suspicious e-mail:

- Call the Help Desk at 995-5513 to report the e-mail.
- Delete the e-mail from your mailbox without clicking on any hyperlinks or attachments.

Follow these rules to create a strong password:

- Passwords must be at least eight characters long.
- Passwords must contain characters from at least three of the following

four categories:

- Uppercase characters (A - Z)
- Lowercase characters (a - z)
- Base 10 digits (0 - 9)
- Symbols found on the keyboard (all keyboard characters not defined as letters or numerals):
` ~ ! @ # \$ % ^ & * () _ + - = { } | [] \ : " ; ' < > ? , . /
- Password may not contain your user account name or any part of your full name.
For example: If your account name is EJE1 and your display name is Jacques, Etienne P., three blocked "tokens" will be created: eje1, Jacques and Etienne. Passwords that contain any of the blocked tokens will not be permitted.
- An old password cannot be re-used. A password history of your previous passwords is maintained. If you try to re-use one of your old passwords, it will not be accepted.
- All these requirements are being enforced for all changed passwords and all newly created passwords.

The County also enforces a password lockout policy. Your User Account will be locked after five failed sign-on attempts within 15 minutes. Your User Account will be automatically unlocked after 15 minutes.

If you have any problems or questions regarding changing your password, call the Help Desk at 995-5513.

Password creation hints and memory tricks

- Don't use passwords that are based on personal information that can be easily accessed or guessed.
- Develop a mnemonic for remembering complex passwords.
- Use both lowercase and capital letters.
- Use a combination of letters, numbers, and special characters.
- Use different passwords on different systems.

Password manager for desktop PCs

Based on the above criteria and instructions, update or create a new password in the [password manager system](#).

Password manager for laptop users

Laptop users must follow different instructions in order for the new/updated password to synchronize with the laptop encryption software.

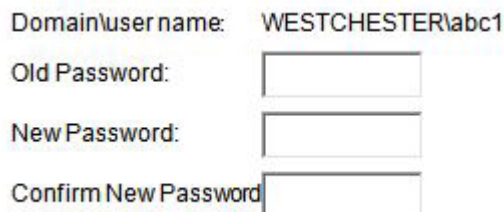
If the steps below for laptops are not followed, the next attempt to sign in will fail.

Also, after three attempts to sign in with an incorrect password, laptop users will be locked out of the system and will have to call the Help Desk at 995-5513 for assistance.

- Your laptop **MUST** be connected to the Westchester County network.
- Sign in to your workstation using your current password.
- Press CTRL + Alt + Delete.
- Click on Change Password.
- Enter your current password in the Old Password field.
- Enter a New Password.
- Re-enter the new password and then submit.

Password manager for both internal and external users via webmail.westchestergov.com/owa, internally and myaccess.westchestergov.com, externally.

- Connect and sign in to Westchester County Webmail
- In the upper right hand corner select "Options"
- From the left navigation, select "Change Password" to arrive at the
- The Change Password page contains the fields below.



The screenshot shows a web form for changing a password. It has four labels on the left and three corresponding text input fields on the right. The labels are 'Domain\user name:', 'Old Password:', 'New Password:', and 'Confirm New Password'. The first input field contains the text 'WESTCHESTER\abc1'. The other two input fields are empty.

| | |
|----------------------|--------------------------|
| Domain\user name: | WESTCHESTER\abc1 |
| Old Password: | <input type="password"/> |
| New Password: | <input type="password"/> |
| Confirm New Password | <input type="password"/> |

- Enter your existing/old password
- Enter your new password
- Then re-enter the new password in the "Confirm New Password" field.
- Submit/Save the changes.
- After saving the new password, Outlook Web Access may prompt you to sign back in to Webmail.

Westchester County Smartphone Password Policy

To increase the overall security of Westchester County's infrastructure, DoIT has enabled password protection on all County issued smartphone devices.

- Passwords must be at least 6 characters in length. If you forget your password, please call the Help Desk (995-5513) to have a service call opened with the Server group to reset your password.
- Passwords must be changed every 90 days.
- If ten incorrect passwords are entered in a row, all data is erased on the smartphone and the device will be disabled. Phone functionality will be disabled as well. To resolve a disabled smartphone device, a service call will need to be opened to schedule a time for the Workstation Group to rebuild the device and reconnect it to the server.

10. Remote Access

DoIT provides VPN access to the County network to facilitate effective work while away from County premises. Access and assigned equipment are provided only by DoIT upon request of Department Managers and are intended for County business purposes only. Use of remote access is subject to this policy and additional restrictions and procedures.

Access to the County's web-based e-mail services, from myaccess.westchestergov.com, is subject to the same policies covered above. Remote access through the myaccess portal also requires dual-factor authentication. Passwords used for these services must also be handled according to County policies and may not be stored in your local computer. Employees are also prohibited from copying County data obtained through the portal onto the local computer/hard drive, or any unauthorized third-party hosting solution (e.g., Dropbox, Google Drive, etc.). In addition, remote access to the County's web-based services, using non-County equipment such as kiosks or computers located in hotel business centers and local libraries, must be terminated before leaving the terminals.

11. Removable Media & Encryption

To minimize the risk of loss or exposure of Sensitive Personally Identifiable Information (PII) maintained by Westchester County and to reduce the risks associated with exposing the County to malware infections, virus attacks, system compromise, interruption of services and legal issues, the County has established an encryption policy that applies to removable media (any device that is capable of storing data that is readily portable and easily removed from the primary computer or other storage device).

This policy applies to all Westchester County employees and other individuals with access to the County network and provides specific guidelines for encrypting information stored on removable media, thereby preventing Sensitive PII from being intercepted by unintended recipients.

In addition, Westchester County does encrypt credit card data received via various e-commerce applications. The County also encrypts PC laptop drives to prevent third parties from accessing the PC should the device become lost or stolen. Electronic communications systems are, however, not routinely encrypted on a countywide basis. Employees must be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed and stored by others.

12. Use of Outside Technology

County employees are not permitted to use their own technology assets on the County network without the express approval of the Chief Information Officer. Examples of such assets include but are not limited to smartphones, tablets, printers, etc. DoIT is not responsible for supporting unapproved devices, and it is prohibited for all County employees to pose additional security risks to the organization through their unauthorized use. Also, if an employee is working with a vendor that needs to connect into the County network, the vendor is required to annually submit an access request form and meet the County's security requirements to ensure the security of the County's infrastructure.

13. Technology Inventory

In order to be certain that each County Department has an accurate list of its current inventory of computer equipment, each Department is required to inventory all computer or related equipment and cross reference this inventory list with the Department of Information Technology to ensure that each computer, printer, and other related equipment has been accounted for in the County. Before a computer or other IT equipment is replaced, removed or transferred, the DoIT Asset Management Group must be contacted at DoITAssetManagement@westchestergov.com so that DoIT can maintain an accurate inventory of equipment and equipment locations. Departments are not permitted to move, change or modify county assets on their own. DoIT is the only authorized entity to do that work.

14. PC Software

The installation of software is the responsibility of the Department of Information Technology. The County has the right to audit County personal computers/laptops and remove any unauthorized software. DoIT must be contacted when loading of software is required. DoIT will need to confirm how the software was purchased to ensure that it is lawfully licensed to Westchester

County and meets all security standards and requirements.

15. Management, Retention and Disposition of Records

Under the guidance of the Chief Information Officer (CIO), all departments and agencies of County government are responsible for the proper management, retention and disposition of their records.

Please refer to Executive Order No. 5 of 2008 on the Proper Management, Retention and Disposition of County Records for complete details regarding statutory and regulatory requirements, and further recommendations on how to comply. The Executive Order can be found on the County's intranet site under Office of the CE → Executive Orders or by clicking here:

http://cww.westchestergov.com/executiveOrders/2008/exec_order_5_001.PDF.

16. E-mail and Communications Activities

Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, malicious links, phishing scams, etc.

The following e-mail and communications activities are not allowed due to associated security risks:

- 16.1. Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam);
- 16.2. Any form of harassment;;
- 16.3. Unauthorized use, or forging, of email header information;
- 16.4. Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies;
- 16.5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type;
- 16.6. Use of unsolicited email originating from within the County's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the County or connected via the County's network;
- 16.7. Posting the same or similar non-business-related messages to other communications platforms.

17. Physical Security

Employees entrusted with Westchester County computer assets, including desktops, laptops and software, must exercise due diligence at all times to prevent theft, destruction or other misuse of the assets. Portable laptops, notebooks, smartphones, and other transportable computers containing sensitive County information must be treated with the same care provided to company documents.

18. Preventing Identify Theft and Data Loss

There are several steps that must be taken to reduce the possibility that confidential personal information in County hands will end up in the hands of identity thieves, including, but not limited to:

- 18.1. Not moving County data to non-County equipment or unauthorized external, third-party hosting services (e.g., Dropbox, Google Drive, etc.) without prior written approval from the Commissioner and Chief Information Officer.
- 18.2. Not copying a whole database with confidential personal information, even to a County PC or laptop. Such data should stay in the secure Data Center. The databases of public records, especially those in the County Clerk's Office, present special problems since these are required to be public. As the County has done in the past, it will continue to encourage and assist the County Clerk in redacting Social Security numbers from the images of those public records.

Refer to the Westchester County Department of Consumer Protection's website for more information on protecting yourself from identity theft:

<http://consumer.westchestergov.com/id-theft>.

19. Vendor Licensing Agreements

All personal computer system software installed on County equipment must comply with the appropriate licensing protocols and copyrights relevant to that software.

Any duplication of copyrighted software is a violation of the Federal copyright law. Under Federal copyright law, County owned software that is loaded on a hard disk may not be duplicated for use on any other PC. The County does not allow any unauthorized copying of software.

20. Telecommunications and Portable Productivity Tools

Westchester County supports the use of telecommunications technology and portable devices (e.g., smartphones, tablets, cell phones, aircards) which meet the County's security requirements and follow accepted use guidelines outlined here. It is the purpose of this section to identify the policies regarding the acquisition and proper use of these devices.

County Phones: Desk Phones

- 20.1. Telephone numbers that are listed or otherwise made known to the public should be answered quickly either by an individual or through an approved voice-messaging system. If the latter is used and voice-messages are recorded, then a responsible individual(s) should check the messages on a routine basis and make appropriate responses to the callers.
- 20.2. Telephone calls should be answered in a courteous and professional manner.
- 20.3. Each Commissioner or Department Head shall take steps to prevent telephone abuse. To assist, DoIT produces telephone utilization reports, which are available through the Telephone Utilization and Billing Information application on the County's Intranet. They should be used to look for patterns of telephone abuse.
- 20.4. If a desk phone is reassigned to another individual, the department should notify Telecom as soon as possible.
- 20.5. Directory assistance from outside operators is restricted because it is expensive and usually not necessary.
- 20.6. MACs (moves/adds/changes) of phones and phone lines for the department should be requested by e-mail to the Telecommunications Team.
- 20.7. Desk phone rental and usage charges are internally billed back to departments.

Portable Devices: Cell Phones, Smartphones, Tablets and Aircards

- 20.8. All Commissioners and Deputy Commissioners are authorized to acquire a cellular telephone. Payment for the acquisition and utilization of the cellular phone shall be funded by the Department.
- 20.9. Requests for portable devices should be signed off by the requesting Department's Commissioner and acknowledged by the end user that the device will be used for County business purposes. Cellular device requests should be submitted to Telecommunications for authorization and processing. Tablet requests should be submitted to the Desktop Asset Manager in DoIT, also for authorization and

- processing.
- 20.10. Cellular charges for device usage are billed directly to the department by the contracted carrier. Use should be restricted, with limited exception for personal emergencies, to County business.
- 20.11. Lost/stolen/broken devices replaced by a user more than three times may result in immediate suspension of service for that individual.
- 20.12. See section 9 ("Identification & Passwords") for details regarding the County's smartphone password policy.

Faxing from Multi-Function Devices (MFDs):

- 20.13. Fax capability from the County's multi-function devices (Xerox - Printer/Copier/Fax) is available in most County departments. Most fax needs can be satisfied by using RightFax, a system that allows users to send and/or receive documents from their departments' multi-function device or from their PC. We encourage the use of RightFax when possible.

21. Contact Information

Submit all inquiries and requests for future enhancements to the owner at:

Marguerite Beirne, CIO
Reference: WC-P08-001
Westchester County Department of Information Technology
148 Martine Avenue, Room 313
White Plains, NY 10601
Phone: (914) 995-8161
Email: mcb1@westchestergov.com

22. Revision History

This policy shall be reviewed at least every year to ensure relevancy.

| Date | Description of Change | Reviewer |
|-------------|----------------------------------|-----------------|
| 01/01/2008 | Original policy release | Scott Fernqvist |
| 10/19/2022 | Various updates and reformatting | Scott Fernqvist |